
THE POWER OF BEING UNDERSTOOD
AUDIT | EXPERTISE | CONSEIL
RSM
IT & Risk Advisory Services
DORA : Digital Operational Resilience Act
Une nouvelle ère dans la régulation numérique

Edito

Au sein de RSM, grâce à nos services de cybersécurité et de résilience, nous aidons les organisations à avoir confiance dans les systèmes, la conception et les données, afin qu'elles puissent apporter des changements transformationnels et permettre l'innovation en toute confiance.

Au sein du département IT & Risk Advisory (ITRA), nous accompagnons divers acteurs de différents secteurs dans leur transformation de résilience numérique, en concevant, mettant en œuvre et évaluant l'efficacité de leurs programmes liés aux risques informatiques.

Nous nous efforçons également d'adapter notre approche de réflexion à mesure que l'environnement réglementaire des différents secteurs évolue, tout en anticipant et renforçant la résilience numérique de nos clients.

Avec l'adoption de DORA, nouveau règlement européen, dont nous dévoilons les différentes particularités à travers les slides suivantes, nous voyons de grands avantages pour les entités financières à disposer d'un cadre harmonisé et complet pour leur résilience. Non seulement DORA apporte des synergies au niveau de l'UE, mais elle a également le mérite de pousser à l'adoption d'un marché unique numérique pour les services financiers.

Qu'est-ce que DORA ?

Le Digital Operational Resilience Act (DORA), directive européenne, instaure des normes cohérentes concernant le risque cyber au sein des institutions financières de l'Union européenne.

01

Qu'est ce que DORA ?

« DORA » vise à établir des exigences uniformes concernant la sécurité des réseaux et des systèmes d'information en vue d'atteindre un niveau élevé de résilience opérationnelle numérique. Ratifiée , cette loi sera mise en œuvre en 2025.

02

Quel est son objectif ?

DORA a pour objectif d'établir un ensemble uniforme de règles visant à renforcer toutes les institutions financières, les préparant ainsi à faire face à diverses perturbations et menaces liées aux technologies de l'information et de la communication (TIC), notamment les cyberattaques.

03

Pourquoi est-ce important ?

DORA élargit la réglementation pour englober les risques associés à une interconnexion croissante, à la transition vers les services financiers numériques et à la dépendance envers des services de tiers. De plus, il préconise une approche prudentielle uniforme au sein d'un marché unique.

04

Résilience numérique ?

La résilience opérationnelle numérique se réfère à la capacité d'une organisation à maintenir ses opérations malgré des perturbations informatiques. Cela implique la prévention, la préparation et la réponse efficace aux incidents tels que les pannes, les cyberattaques, afin d'assurer la continuité des services et une récupération rapide.

A qui s'applique la loi DORA?

Fondamentalement , tous les acteurs des marchés financiers sont concernés par DORA. Les règles DORA sont destinées à couvrir un très large éventail d'entités de services financiers, avec des exigences appliquées proportionnellement en fonction de la taille et du profil de l'entreprise. Voici une liste non exhaustive des entités couvertes par DORA :

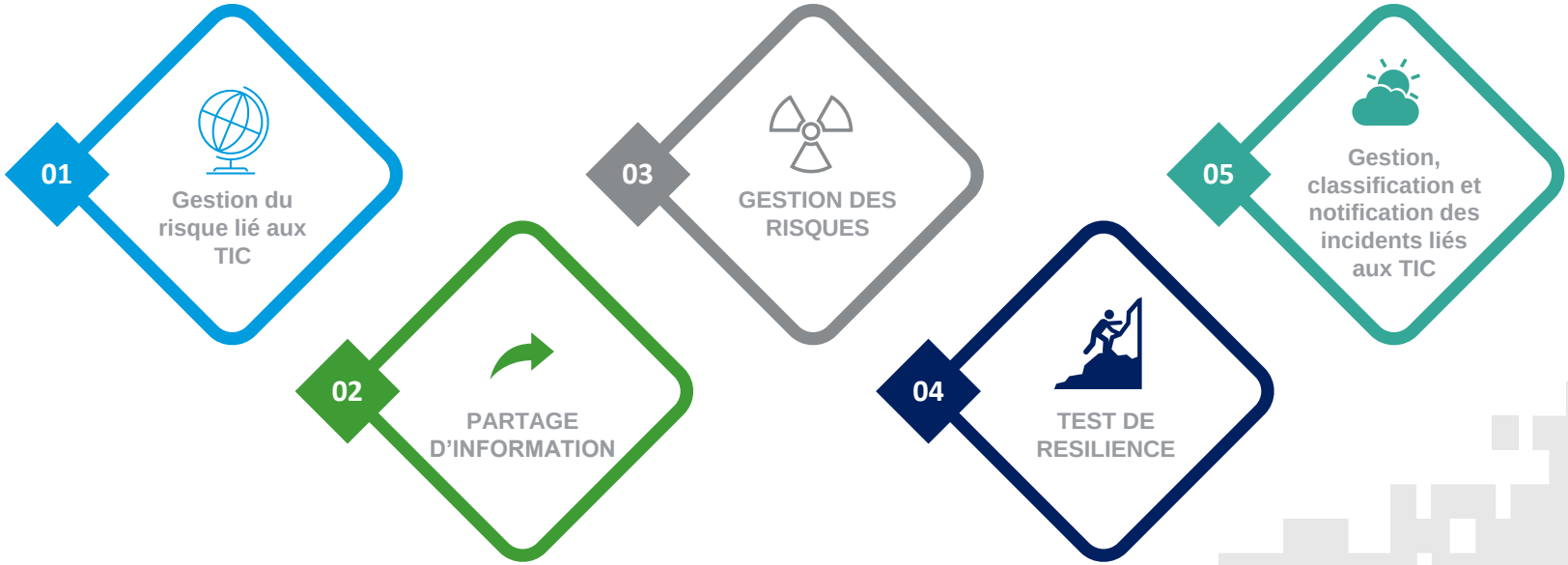
Les entités concernées
• Établissements de crédit • Gestionnaires de fonds d'investissement et sociétés de gestion • Établissements de paiement et établissements de monnaie électronique • Cryptoactif • Dépositaires centraux • Plateformes de trading • Fournisseurs de services informatiques • Compagnies et intermédiaires d'assurance et de réassurance • Institutions de retraite professionnelles • Agences de notation • Administrateurs de benchmarks critiques • Commissaires aux comptes et cabinets d'audit • ....

Quelles sont les thématiques ?

DORA vise à simplifier et à mettre à jour les règles de gestion des risques liés aux TIC. Cela comprend :

- un accent sur les rapports d'incidents, les tests de résilience opérationnelle numérique,
- le partage d'informations et la gestion des risques liés à la chaîne d'approvisionnement des tiers.

Les principales exigences et considérations au sein de DORA sont résumés en cinq grands thèmes.



Qu'est-ce que cela signifie pour vous ?

Comment vous accompagner ?

Réglementation appliquée

De même, DORA représente un nouvel ensemble de réglementations significatives qui requièrent une conformité stricte. Il sera accompagné d'un mécanisme d'application, tel qu'un contrôle externe ou des sanctions pouvant atteindre « 1 % du chiffre d'affaires »

De la gestion du risque opérationnel à la résilience opérationnelle

Avec l'évolution significative de l'environnement réglementaire et un renforcement de la surveillance, même les organisations bien établies doivent reconnaître la possibilité d'une transformation afin de garantir la conformité.

Notre proposition d'accompagnement :

CADRAGE

Définir la portée de DORA sur votre entité
Identifier les parties prenantes clés
Structurer les ateliers

ASSESMENT

Audit de votre entité pour définir votre niveau de compliance avec recommandation
Identifier les impacts et les actions en lien avec DORA sur votre entité

MISE EN PLACE DES RECOMMANDATIONS

Mise en œuvre du plan d'action
Suivi et Evaluation

Développer une culture du risque cyber au sein de votre entité

Quelques exemples

Comprendre les obligations est la clé d'une bonne transformation. RSM vous aide à identifier les problèmes liés à la cybersécurité, à la continuité des activités et à l'audit informatique . Cette expertise nous permet de vous accompagner sur tout le périmètre DORA.

Gestion du risque lié aux TIC	Nous utilisons les normes ISO27002 et EBIOS pour cartographier les risques et mettons en place un Système de Management de la Sécurité de l'Information (SMSI) basé sur ISO27001 pour assurer une maîtrise efficace de ces risques. Notre expertise vous accompagnera à chaque étape.
Partage d'informations	Nous encourageons la collaboration entre les entités pour progresser collectivement dans la gestion des risques cyber. Nous proposons des solutions telles que l'intégration dans des clubs de sécurité, la mise en place de dispositifs de veille cyber, et d'autres moyens de renforcer la collaboration pour une cybersécurité plus robuste.
Gestion des risques	Nous proposons notre expertise pour vous aider à élaborer une politique de sécurité pour les tiers et une procédure de sélection des fournisseurs intégrant des contrôles de sécurité adéquats, vous permettant ainsi de maîtriser la sécurité de vos partenaires externes.
Test de résilience	Nous soulignons notre expertise dans la construction de programmes annuels de tests de résilience, incluant les pentests et les plans de continuité d'activité (PCA). De plus, nous sommes en mesure de vous accompagner dans la réalisation de ces tests pour garantir la robustesse de votre sécurité.
Rapports d'incidents	Nous vous accompagnons à inventorier tous les incidents de sécurité et à établir des mécanismes de notification conformes aux exigences de l'ANSSI. Nous sommes là pour mettre en place les procédures nécessaires et les outils appropriés pour assurer votre conformité.

Les éléments essentiels pour réussir

Anticiper et définir votre stratégie

Commencer dès que possible en impliquant les intervenants pertinents dès le départ avec un sponsor DORA.

Effectuer un pre-assesment

Conduire une évaluation DORA pour anticiper la conformité et renforcer la résilience opérationnelle numérique de votre organisation..

Promouvoir la culture du risque

Sensibiliser les acteurs aux enjeux de la sécurité informatique et mettre en place des pratiques de gestion des risques adaptées.

Se projeter avec vos Tiers TIC

DORA change la relation avec les tiers TIC en imposant des normes de sécurité plus strictes.

Dédier un budget et des ressources

Un défi récurrent lié à la gestion budgétaire et à la disponibilité des experts clés pour DORA.

Jean-Philippe ISEMANN
Associé/ Partner
CISA, CISM, CRISC
+33 6 61 8748 99
jean-philippe.isemann@rsmfrance.fr
www.linkedin.com/in/jpisemann/fr

RSM France

26, rue Cambacérès
75008 Paris
T : +33 (0)156 88 3120

www.rsmfrance.fr